REMARKS

[0010] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1-9, 12, 15-17, 19-31, 34-36, 38, 39, 41 are currently pending
- Claims 1, 16, 20 and 39 are amended herein

[0011] Support for the amendments to claims 1, 20 and 39 is found in the specification at least at pages 27-29.

Claim Objections

[0012] Claim 39 stands objected to for the following informalities: "one of more of." Claim 39 includes appropriate correction, therefore Applicant respectfully requests the Examiner to withdraw the claim objection.

Cited Documents

[0013] The following documents have been applied to reject one or more claims of the Application:

- Clifton et al, "Developing Custom Intrusion Detection Filters Using Data Mining", IEEE 2000.
- Cuppens, "Managing Alerts in Multi-Intrusion Detection Environment", IEEE 2001.
- Denning, U.S. Patent No. "An Intrusion Detection Model", IEEE 1987.

- Vikaykuman, U.S. Patent No. 5,745,896.
- Greifeneder, U.S. Patent Application Publication No. 2004/0243349.

Claims 1-4, 8-9, 12, 15-17, 19-23, 27-31, 34-36, 38-39, and 41 Are Non-Obvious Over Clifton, in view over Cuppens, and in further view over Denning, and in further view over Vikaykuman.

[0014] Claims 1-4, 8-9, 12, 15-17, 19-23, 27-31, 34-36, 38-39, and 41 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Clifton, in view over Cuppens, and in futher view over Denning, and in further view over Vikaykuman. Applicant respectfully traverses the rejection.

Independent Claim 1

[0015] In light of the amendments presented herein, Applicant submits that the rejection of independent claim 1 is overcome. Specifically, the combination of Clifton, Cuppens, Denning, and Vikaykuman does not teach or suggest, at least, the following claimed features of amended claim 1 (emphasis added):

> **performing cluster analysis to group the at least one message sequence into at least one cluster**, wherein the cluster analysis includes forming a data matrix based on information in the at least one message sequence and forming the at least one cluster based on the data matrix, **at least one cluster includes the reference sequence;**
>
> **sorting into a ranked order at least two clusters based on a number of members associated with each cluster**, the sorting **prioritized from least members to most members** associated each of the at least two clusters; and

outputting the information into **a table format based on the sorting into a ranked order, each cluster represented in the table format is linked to information regarding an associated message sequence**

[0016] Claim 1 recites in part, "performing cluster analysis to group the at least one message sequence into at least one cluster... at least one cluster includes the reference sequence." The Office cites Cuppens, 4.1-4.2.3 as teaching this element. (Action, p. 6.) According to the Office, Cuppens describes "performing cluster analysis to identify cluster alerts from data in its relational database and forming at least one cluster based on the data matrix (e.g., relational database)." (Action, p. 6). Applicant respectfully asserts that "cluster analysis to identify cluster alerts from data in its relational database" of Cuppins does not teach or suggest "performing cluster analysis to group the at least one message sequence into at least one cluster, wherein the cluster analysis includes forming a data matrix based on information in the at least one message sequence and forming the at least one cluster based on the data matrix, at least one cluster includes the reference sequence".

[0017] The Office does not rely on the other cited documents to teach "performing a cluster analysis" as recited in claim 1, because cited documents Clifton, Denning and Vikaykmuan fail to teach or suggest "performing cluster analysis" as recited in claim 1.

[0018] Further, Applicant submits that the combination of Clifton, Cuppens, Denning, and Vikaykuman fails to teach or suggest, at least, the following features of claim 1 which have not been considered (emphasis added):

sorting into a ranked order at least two clusters based on a number of members associated with each cluster, the sorting prioritized from least members to most members associated each of the at least two clusters; and

outputting the information into **a table format based on the sorting into a ranked order, each cluster represented in the table format is linked to information regarding an associated message sequence**

[0019] Consequently, the combination of Clifton, Cuppens, Denning, and Vikaykuman does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 20

[0020] In light of the amendments presented herein, Applicant submits that the rejection of independent claim 20 is overcome. Specifically, "performing cluster analysis to identify and cluster alerts from data in its relational database" as allegedly discussed in Cuppens does not teach or suggest the claimed, "cluster analysis logic configured to perform cluster analysis to group the at least one message sequence and the reference message sequence into at least one cluster… the cluster analysis logic is configured to measure a distance between two or more message sequences of each cluster formed by the cluster analysis logic." (Action, p. 10).

[0021] Further, Applicant submits that the combination of Clifton, Cuppens, Denning, and Vikaykuman fails to teach or suggest, at least, the following features of claim 1 which have not been considered (emphasis added):

output logic configured to **output** the information **as a two-dimensional presentation of the at least one cluster and indicating the reference sequence and the distance associated with the at least one message sequence**

[0022] The Office rejects claim 20 on similar grounds as those provided for claim 1. Without needlessly repeating the discussion above in regard to amended claim 1,

Applicant asserts that amended claim 39 is allowable at least for similar reason as those discussed regarding amended claim 1. Consequently, Clifton, Cuppens, Denning, and Vikaykuman does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 39

In light of the amendments presented herein, Applicant submits that the rejection of independent claim 39 is overcome. Specifically, "performing cluster analysis to identify and cluster alerts from data in its relational database" as allegedly discussed in Cuppens does not teach or suggest the claimed, "means for performing cluster analysis to group the at least one message sequence and the reference message sequence into at least one cluster." (Action, p. 15).

[0023] The Office rejects claim 39 on similar grounds as those provided for claim 1. Without needlessly repeating the discussion above in regard to amended claim 1, Applicant asserts that amended claim 39 is allowable at least for similar reason as those discussed regarding amended claim 1. Consequently, Clifton, Cuppens, Denning, and Vikaykuman does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Dependent Claims 2-4, 8, 9, 12, 15-17, 19, 21-23, 27-31, 34-36, 38 and 41

[0024] Claims 2-4, 8, 9, 12, 15-17, 19, 21-23, 27-31, 34-36, 38 and 41 ultimately depend from independent claim 1 or 20. As discussed above, claims 1 and 20 are allowable over the cited documents. Therefore, claims 2-4, 8, 9, 12, 15-17, 19, 21-23, 27-31, 34-36, 38 and 41 are also allowable over the cited documents of record for at

least their dependency from an allowable base claim. These claims may also be allowable for the additional features that each recites.

Claims 5-7, and 24-26 Are Non-Obvious Over Clifton, in view over Cuppens, and in further view over Denning, and in further view over Greifeneder

[0025] Claims 5-7 and 24-26 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Clifton, in view over Cuppens, and in further view over Denning, and in further view over Greifeneder. Applicant respectfully traverses the rejection.

Dependent Claims 5-7 and 24-26

[0026] Claims 5-7 and 24-26 ultimately depend from independent claim 1 or 20. As discussed above, claims 1 and 20 are allowable over the cited documents Clifton, Cuppens, Denning, and Vikaykuman. Therefore, Applicant respectfully asserts that claims 5-7 and 24-26 are also allowable over the cited documents of record for at least their dependency from an allowable base claim and because the cited document Greifeneder fails to compensate for the deficiencies of Clifton, Cuppens, Denning, and Vikaykuman in regard to claims 1 and 20 as discussed above. These claims may also be allowable for the additional features that each recites.

Conclusion

[0027] Applicant submits that all pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned representative for the Applicant before issuing a subsequent Action.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/Jacob S. Scott/ Dated: 2009-June-15

Jacob S. Scott (Jake@leehayes.com; (509) 944-4728)
Registration No. 62,806

John Meline (Johnm@leehayes.com; (509) 944-4757)
Registration No. 58,280

Customer No. **22801**

Facsimile: (509) 323-8979
www.leehayes.com